Генератор псевдослучайных чисел и его применение в защищенной базе данных

Кузьменок А.Ю.
Научный руководитель: Кренделев С.Ф.

Новосибирск
2014

План

- Идея генератора
- Параметры и необходимые условия
- Модификация
- Применение
- Статистическое тестирование
- Скорость генерации
- Заключение

Идея генератора

Пусть необходимо найти корни уравнения

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m = 0, a_i \in Z \quad (1)$$

Один из способов:
представление решение в виде p-адического числа

$$x = t_0 + t_1 p + t_2 p^2 + \ldots, \quad (2)$$

где $t_i \in \{0,1,2,\ldots, p-1\}$, а p – простое.

Необходимые условия и параметры генерации

Ключ генератора:

набор коэффициентов a_i и начальный корень x_0 сравнения $f(x) = 0$.

Условия генерации:

1) $f(x) = 0$ имеет корень x_0 по модулю p

2) $f'(x_0)$ обратима по модулю p

3) $f(x) = 0$ имеет вещественные или комплексные корни

Модификация

Пусть коэффициенты a_i уравнения

$$f(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m = 0, a_i \in Z \qquad (1)$$

также являются p-адическими числами:

$$a_i = a_{i0} + a_{i1} p + a_{i2} p^2 + \ldots,$$

и удовлетворяют уравнениям:

$$a_i^2 + b_i = 0, b_i \in Z$$

Применение
Шифрование на основе арифметического кодирования

- Генерация случайных разбиений отрезка

Применение
Гомоморфное шифрование

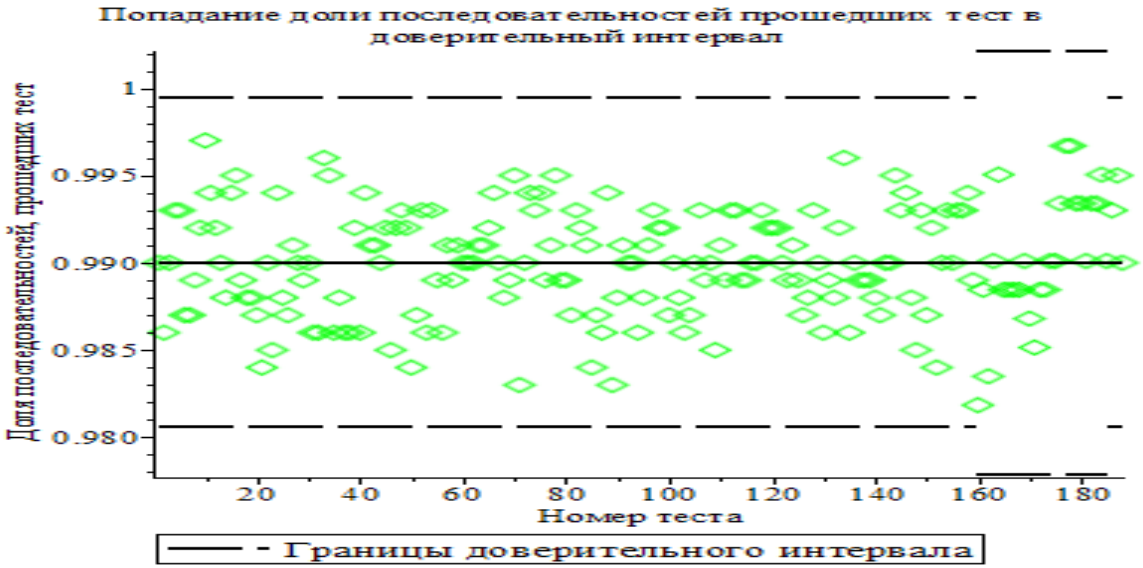
- Генерация ключей шифрования
- Генерация случайных коэффициентов в процессе шифрования

Применение
Матричное шифрование

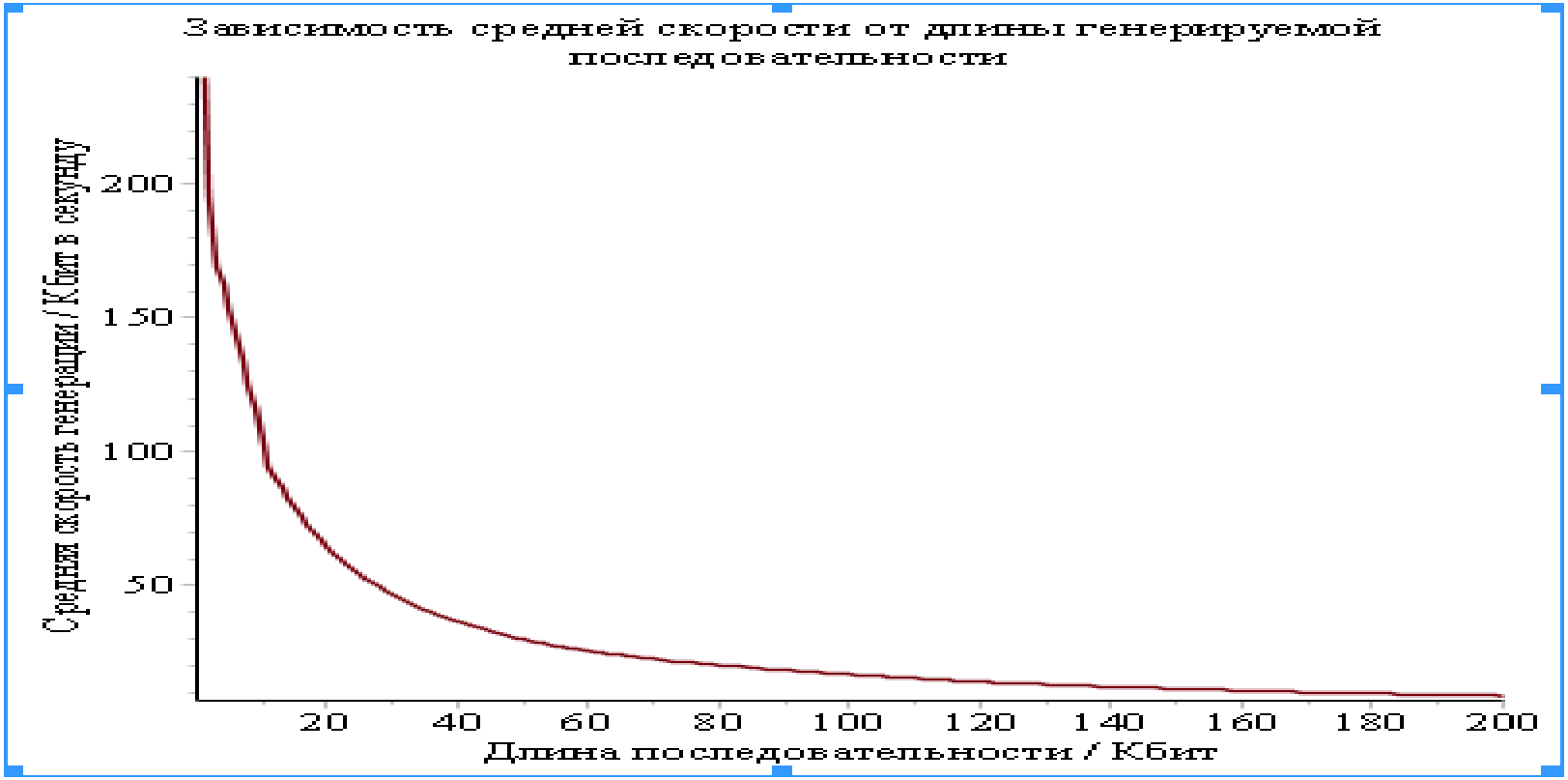
- Генерация элементов секретных матриц
- Генерации секретного обхода матрицы
- Генерации коэффициентов монотонной функции

Статистическое тестирование

- NIST STS
- Последовательности длинной 1 миллион бит
- Размер выборок 500, 1000



Скорость генерации



Заключение

- Отсутствие периода
- Простота инициализации
- Хорошие статистические свойства

Пакет статистического тестирования NIST STS

- Набор статистических тестов NIST STS разработан Национальным институтом стандартов и технологий США.
- Выбор данного пакета обусловлен тем, что он имеет большую криптологическую направленность, которая достигается путем введения в пакет таких тестов, как проверка линейной сложности и универсального теста Маурера.

p-адические числа

Целым p-адическим числом для заданного простого p называется бесконечная последовательность $x = \{x_1, x_2, \ldots\}$ вычетов по модулю p, удовлетворяющих условию:

$$x_n \equiv x_{n+1} (\mathrm{mod}\ p)$$